学校编码：**10384**　　分类号 _____ 密级 _____

学号：**19020061151734**　　**UDC**_____

厦　门　大　学

硕　士　学　位　论　文

一种基于链式环签名的安全电子投票

A Secure Electronic Voting Based on Linkable Ring Signature

何 滨

指导教师姓名： 曾 吉 文教授

专 业 名 称： 基础数学

论文提交日期： 2009 年 5 月

论文答辩日期： 2009 年　　月

学位授予日期： 2009 年　　月

答辩委员会主席： _____

评　　阅　　人： _____

2009 **年** 5 **月**

厦门大学学位论文原创性声明

兹呈交的学位论文，是本人在导师指导下独立完成的研究成果．本人在论文写作中参考的其它个人或集体的研究成果，均在文中以明确方式标明．本人依法享有和承担由此论文而产生的权利和责任．

声明人（签名）：

年　　月　　日

厦门大学学位论文著作权使用声明

本人完全了解厦门大学有关保留、使用学位论文的规定.厦门大学有权保留并向国家主管部门或其指定机构送交论文的纸质版和电子版，有权将学位论文用于非赢利目的的少量复制并允许论文进入学校图书馆被查阅，有权将学位论文的内容编入有关数据库进行检索，有权将学位论文的标题和摘要汇编出版．保密的学位论文在解密后适用本规定.

本学位论文属于

1、保密（　　），在　　年解密后适用本授权书.

2、不保密（　　）.

（请在以上相应括号内打”✓”）

作者签名:　　日期:　　年　月　日

导师签名:　　日期:　　年　月　日

目　录

Contents

摘　　要

电子投票以密码学为基础，运用计算机和网络技术来实现。选举管理机构可以不必象人工选举那样进行大量的人工选票发放和选票的统计工作，投票人也不必到固定的投票中心去投票。与传统人工投票方式相比，电子投票可大量减少人为因素，做到更公平、更安全、更高效、更灵活。并且对电子投票中涉及的密码学理论与实际应用问题的研究对电子安全领域其他方面也具有一定的借鉴作用。所以对电子投票进行研究具有一定的理论意义与实际应用价值。如何充分利用电子投票的优势，设计出更具安全性、实用性的电子投票方案，也成为目前安全领域学术届研究的一个热点问题。

本文完成的工作主要有以下几个方面：

1. 介绍了电子投票所涉及的一些密码学理论，阐述了安全电子投票所应具备的几条基本性质，然后对一些具代表性的安全电子投票方案进行深入分析，发现某些现有安全电子投票方案存在安全性和操作性上的缺陷。

2. 本文提出了一个基于身份的链式环签名来实现的安全电子投票方案。该方案实现了投票者身份的匿名性，投票的唯一性、完整性、准确性、公正性和可验证性。本方案关键在于解决了在电子投票方案中由于管理中心或群管理者权利过大造成投票者身份泄露的问题，可以无条件保证投票者身份的匿名性。其次，采用链式环签名可使方案的流程简化，大大提高了效率，并且环签名本身性质保证了投票者身份的匿名性。再者，弃权的投票者不必投一张空白的选票，任何人无法冒充投票者进行投票。最后，针对选举中我们可能对自己的投票感到后悔，我们可以利用环签名的可链接性，进行新一轮的投票，用新的选票替代旧的，使自己不会因一时的疏忽和犹豫而投错票。

关键词： 密码学；基于身份的环签名；链接性；电子投票.

Abstract

Electronic voting employs computer and network technologies to realize the voting function, which is based on cryptography. Voting administrator don't have to provide a large number of artificial ballots or carry on the work of counting the ballots and voters don't have to go to the regular voting center. Comparing with the traditional voting mode, electronic voting is more impartial, more secure,more efficient and more flexible, which can reduce man-made factors greatly. Furthermore, cryptography theory and application involving in electronic voting can be used for reference to the other aspects of electronic security fields. Therefore, it is significance to the study of electronic voting.And how to use the advantage of electronic voting thereby designs a more secure and more applicable electronic voting is also a hot issue in the security field.

The main results and contents are as follows.

1.Introduced a number of electronic voting Cryptography Theory,and Secure e-voting should be introduced with a few basic properties.Then a representative of some electronic voting security program to conduct in-depth analysis.Found that certain existing security program of the existence of electronic voting security and operational deficiencies.

2.In this paper, a ring based on the identity of the signature chain to achieve a secure electronic voting program.The program achieved the status of the anonymity of voters, democracy, integrity, accuracy, fairness and verifiability .The key lies in the program to solve the electronic voting program management center or the right group of managers resulted in excessive leakage of the question of the identity of voters,Voters can maintain the identity of unconditional anonymity.Second, the use of the signature chain ring allows the program to simplify the process, greatly improving the efficiency, Central and the nature of the signature itself to ensure the anonymity of the identity

of voters.Third, the voters do not have to abstain from a vote Blank ballots, a person posing as voters can not vote. Furthermore, in view of the election, we might regret their vote, we can use ring signatures can be linked, and a new round of voting, the ballot papers with a new alternative to the old, so he will not because of negligence and hesitation and Cast votes in the wrong.

Key words: Cryptograph;Ring Signature based ID;linkable; Electronic Voting.

第一章 导论

§1.1 研究电子投票的意义

近年来，计算机网络特别是 Internet 在我国有着长足的发展，据统计，我国在 1998 年还只有 210 万因特网用户，到 1999 年底已升至 890 万户，至 2001 年初，我国计算机拥有数量已逾 9300 万台，其中联网计算机已达 890 万台，因特网用户已达 2250 万。之后以飞快的速度增长。从目前看来，互连网络提供的各种便利服务，如网上购物，网络银行，无纸办公，正取代原来的生活方式，为人们喜爱和接受。可以想象，在不远的将来，几乎是我们身边的每一件事情，都可以借助于网络由计算机实现。

投票行为，是现代民主社会中一个经常发生的行为，而不是专属于选举的特殊行为，上至国家领导人选举，下至用餐抉择，都要进行投票。特别是在近来，各类投票活动不断增加，不仅有传统的选举投票，如各级党代会、人大、政协选举；还有其他的评审投票，如各级、各类奖项评审，立项项目评审；再如各级各类十佳、最佳人物、事物评比，人事考评、论文评审、晋级评议等，所有这些活动都是和投票行为紧密联系的。

然而，传统的人工投票方式存在的问题却日益突出：第一，人工记票花费的时间太长。第二，重新记票相当困难。这是因为票箱开封，选票难以重新整集，而且记票时有可能弄脏选票，甚至遗失选票。第三，人力财力浪费严重。投票人都要舟车劳顿到指定的投票站进行投票，这无疑加大了投票的代价，造成了人财力的浪费。在这种情况下，投票行为的实现方式也不可能在这个日新月异的社会环境中停滞不前，于是，电子投票系统便应运而生。

电子投票作为通常投票的电子化，利用先进的网络设施和密码学技术，使选民可以在投票站或自己家中设置的计算机终端通过互联网进行投票，最后的记票工作全部由计算机自动完成，不仅在组织工作、选票搜集与统计方面都节省了大量的人力

物力，而且在一定程度上保证投票人的利益和投票结果的公正，所有这些优点使其取代传统的投票方式成为必然的趋势。现在，计算机互连技术、网络安全、通讯技术的高度发展，以及密码学相关领域的重大突破，使电子投票系统真正大规模应用于投票逐步成为可能。

因此，电子投票具有省钱、省力和安全的特性，而且电子选举中涉及到得密码学的很多问题对于研究其他安全领域的问题也具有推动作用。所以对于电子投票系统的理论和实际研究都是很有意义的。

§1.2 电子投票的研究现状

§1.2.1 电子投票的发展历史

电子投票比传统的人工投票方式高效、方便、灵活，人们很早就积极进行了电子投票系统的探索。最早在 1884 年，大发明家 Tomas Edison 就发明了一种电子投票装置，他想在 Massachusets 市的立法机关中进行电子投票，但没有成功。不过，人们对电子投票的追求一直都没有停止。随着计算机的出现，人们逐步开始利用计算机进行电子投票的研究、实践，提出了很多或成功或失败的电子投票方案，也随之出现了一些电子投票系统。

第一个现代意义上的电子投票方案，是由 Chaum[1] 于 1981 年提出的，它采用公钥密码体制，并利用数字签名花名册来隐藏投票人的身份，但不能无条件的保证投票人的身份被跟踪。之后一些日本学者先后发表了若干关于电子选举的实用方案。后来，随着密码学相关理论的逐渐发展，如盲签名方案的蓬勃发展，国际上众多的学者都开展了这方面的研究工作，出现了许多有关电子选举的理论方案和实用方案。但是这些方案的一个最大弊病在于实用性不强，不适应大型选举。此后，此后电子投票的发展有两个方向，一个是基于同态加密技术的电子投票方案，该技术可以掩盖选票的内容。另一个是基于匿名信道技术的电子投票方案，该技术可以掩盖投票者的身份。

1985 年， Cohen 和 Fisher[9] 提出了基于同态加密技术的电子投票方案，接着 Benaloh, Yung[10], Iversen[11], Sako 和 Kilian[17] 等也分别提出了基于同态加密技术的电子投票方案。这些方案各有优缺点。举例来说， Cohen 和 Fisher 的方案需要分散的组织机构来保护选民的秘密，但要求所有的投票必须同时进行。Iverson 模仿电子货币协议来试着解决这个问题，但其主要缺点是如果所有的机构合谋，则投票者无秘密可言。更重要的是，这些方案使用高次剩余加密技术，需要大规模的传输与计算，不适应大规模的投票。

另一方面，也有一些基于匿名信道的电子投票方案。所谓匿名信道是指不可跟踪电子邮件系统和公告牌等能掩饰信息来源的信道。 Chaum 在匿名信道技术上率先提出不可跟踪电子邮件系统，这个系统在至少一个掩盖者是可靠的情况下，能可靠掩盖信息来源。Chaum 基于匿名信道技术提出了第二类电子投票方案的雏型，尽管单个投票者的失败会影响到整个投票，但该方案保证失败能被追踪到。之后 Chaum[15] 和 Ohta[3] 利用匿名通讯信道分别给出了一个适合于大群体选举的投票方案。这个方案保证了投票者的匿名性，然而都没有解决选票的秘密性和公平性。 Asano[6] 提出的方案解决了公平性问题，但对于腐败的管理者仍是不安全的。随后的方案 [7] 虽然解决了秘密性问题，但又没有解决公平性问题。

以上的投票方案，要么是太复杂，不适合大型投票，要么就是安全方面存在大的漏洞。第一个实用的适合大规模投票的方案，是由 Fujioka, Okamoto 和 Ohta[2] 在 1992 年提出的 Foo 方案，该方案的核心采用了比特承诺技术和盲签名技术。Foo 方案提出后，受到了较大的关注，被认为是一个能较好实现安全投票的电子投票协议。它既保证了选票的秘密性和公平性，也解决了投票者身份匿名的问题。许多大学和公司的研究机构都对其进行了改进，开发出了相应的电子投票软件系统。其中著名的有麻省理工学院 (MIT) 的 EVOX 系统、华盛顿 (Washington) 大学的 Sensus[8] 系统。但是它在安全性方面还存在一些缺陷： 1. 该方案要求弃权者提交一张空白选票。 2. 该方案中，如果两个投票者选取相同的随机密钥及相同的方式投票，那么选

票及其签名就完全一样。计票机构就可能去掉一些重复的选票而伪造出“合法的”选票。3. 该方案使用比特承诺协议虽然保证了选票的公平性，但在计票时如果投票者提供了一个非法的密钥或投票者中途退出，则相应的选票无法打开，计票机构就可能与管理机构相勾结来影响结果。国内，谢金宝 [18] 等人也提出了一个改进方案，用公证人群替代签证人发放匿名的成员证书，这样选民可以直接匿名投票，但公证人群本质上与签证人是一样的，如处理不当，公证人也可伪造成员证书参与投票。

随着密码学中群（环）签名的发展和其他技术的出现，越来越多的应用与电子投票之中，使得电子投票中存在的一些问题得以解决，但仍然存在许多的问题，例如管理机构和群管理者权利过大，在投票过程中存在的腐败和强迫问题。另外，就现有的电子投票系统来说，没有投票人百分百的参与，是无法严格维护最终结果的。所以现阶段，电子投票方面值得我们研究的东西还很多。

§1.2.1 电子投票的研究目标

传统的人工投票方式，使用的是纸质选票，现在的电子投票，前端采用数字化的电子选票。然而，投票的本质却没有发生变化，仍然要求整个投票过程简单、快捷且要做到公开、公平和公正。因此，电子投票系统的主要目标就是：

1. 确保投票人的利益不受侵犯。即任何组织或个人不能从选票信息中提取出投票人的信息，实现真正的匿名投票。

2. 保证投票结果的公正、正确。也就是不能出现伪造选票、涂改选票及有效选票不被正确统计的作弊现象。

3. 高效、快捷、灵活，能减少投票开支。

理想的电子投票系统的目标，就是通过公众网络来完成投票，且以最小的代价满足最多的需求。为此，很多电子投票系统的研究者根据不同的投票情况，对电子投票系统应该满足的最低要求进行了探讨，形成了不同的分类，一般来说，电子投票系统应该满足如下的要求：

1. 准确性 (Accuracy) 任何无效选票都不予计算。无论任何人对选票进行更改、复制或删除，系统都能够检测出来并进行处理，使之不能扰乱正常的投票。

2. 完整性 (Completeness) 验证单位应接受任何合法投票人的投票，所有有效的选票都应该被正确统计。

3. 秘密性 (Privacy) 所有的选票都是保密的，任何人都不能将选票和投票人对应起来以确定某个投票人投票的内容。

4. 唯一性 (Democracy) 只允许合法的投票者进行投票，且其只能投一次。

5. 公正性 (Fairness) 任何事情都不能影响投票结果。即在选举过程中不能泄漏中间结果，从而影响公众的投票情绪及投票动向，以致影响最终的投票结果。

6. 合法性 (legalization) 只有经授权的人才能投票。

7. 可验证性 (Verifiability) 任何投票者都可以检查自己的选票是否被正确统计，任何人都可以对投票结果进行验证。

8. 方便性 (Convenience) 系统应该简单、方便。对投票者来说，投票所需的知识和操作不能太多。

9. 灵活性 (Flexibility) 对投票的人数和场地不应有任何限制。各投票者的投票活动相互独立，不受影响，不需要在同一时间一起参加投票。

10. 效率性 (Efficiency) 投票者可以自主安排自己的投票过程。即投票完成前的所有计算，都应保持在一个合理的范围内，以致投票者不需要等待其他投票者就可以完成他的流程。

11. 非强制性 (Non-mandatory)[12] 投票者自己对选票进行填写，投票之后不可以向强制者或购票者证明他的投票内容。这主要是为实际应用考虑，即考虑投票人的投票行为是否出于自由意识，或是受到暴力威胁及受到贿票的利诱。

12. 广义可验证性 (Universal Verifiability) 任何感兴趣的第三方可以验证所有选票的合法性和投票结果的公正性。

其中 1-7 条为实现安全电子投票协议必须的安全性要求，任何电子投票协议都必须满足这 7 条协议，第 8-9 条使电子投票协议具有更大的实用性。第 10 条将增加电子投票协议的效率，并可以提高协议实用性。第 11-12 条可防止投票中的犯罪行为，使电子投票协议更具普遍性。

§1.2.1 电子投票研究中存在的问题

随着计算机网络的飞速发展和普遍应用，网络安全问题已成为政府，企业及广大网络用户最关心的问题之一。虽然计算机网络安全的涉及面很广，但是计算机网络提供的最基本功能仍然是网络站点之间的数据交换。因此数据传输的准确性、机密数据的保密性以及建立在底层数据传输基础上的会议协议的完善成为关键问题。电子投票是一种网络化和信息化的活动，上述网络安全问题的概念也适用与电子投票系统。因此一个好的电子投票系统，不仅取决于它所选择的数据保密算法的可靠性，而且也离不开投票信息流程协议设计的完善程度。

与常见的网上调查不同，电子投票系统需要对许多信息进行保密，甚至对系统管理员都要保密，这就决定了电子投票协议属于现代密码学的范畴。一个电子投票方案可通过签名或别的密码技术来实现。随着密码学相关理论的逐渐发展，国内许多学者利用不同的密码技术相继地提出一些方案。当然各方案也存在着不同的安全问题。

一般地，投票者的主观意愿和投票的方法都能影响投票结果。目前一些方案中还存在这些问题：

1. 不能防止一票多投。

2. 投票者对投票机构来说是透明的，没有保证匿名性。

3. 不能解决“选票碰撞”的问题。如果两个投票者使用相同的随机密钥及相同的方式投票那么选票及其签名就完全一样。这时计票机构有可能去掉一些重复的选票而伪造另一些合法的选票，却不被投票者察觉。

4. 不能防止“投票者中途退出”问题。